Statement

Of

Robert N. McFarland

Assistant Secretary for Information and Technology

Department of Veterans Affairs

Before the

Subcommittee on Oversight and Investigations

Committee on Veterans' Affairs

U.S. House of Representatives

October 6, 2004

Thank you, Mr. Chairman. I am very pleased to appear before this Committee representing the Secretary and the Department's information technology programs. On March 17, 2004, I appeared before this Committee and gave you an overview of VA's information technology processes and projects. I am here today to provide you with an update regarding VA's Authentication and Authorization Infrastructure Project (AAIP). We currently have the Department positioned almost 12 months ahead of the mandates contained in Homeland Security Presidential Directive12 (HSPD-12), titled "Policy for a Common Identification Standard for Federal Employees and Contractors." VA has achieved this position, which is well ahead of many agencies, because we have continuously synchronized AAIP with government deliberations and involvement in the process that lead up to HPSD-12. We view this as a success story. Events continue to validate the merits of the AAIP approach taken by VA, and the Department continues to display substantial leadership in the Federal arena.

Currently, VA has a Federal Manager's Financial Integrity Act (FMFIA) "material weakness" related to account management. AAIP plays a significant part in addressing this issue by creating better account management controls, two factor authentication with smart cards, and a reduction on the reliance of static passwords. The VA's Office of Inspector General (OIG) has reviewed AAIP, and believes that it is a significant move toward removing this outstanding concern.

AAIP specifically considers, and sets up strategies to effectively comply with, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security

Rule, the Gramm Leach Bliley Act for financial services, the E-Government Act of 2002, including the Federal Information Security Management Act (FISMA) provisions, and OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies, as well as the OMB memo entitled Streamlining Authentication and Identity Management within the Federal Government. As such, AAIP will make a significant, cost-effective contribution to VA's commitment to achieve regulatory compliance.

The benefits of AAIP were apparent in preliminary tests with the Drug Enforcement Agency (DEA), wherein AAIP demonstrated the ability to save up to 45 minutes in processing time associated with pharmacy transactions. This can be achieved through the application of digital signature, which complies with DEA regulations, reduces paperwork, and substantially reduces unintended errors. In the process, service to the veteran is greatly enhanced in a cost effective manner.

During detailed testing of smart card usage in a "thin client" environment, AAIP demonstrated the ability to recover up to 45 minutes per day of clinician time through simplified logon processes. VHA has tens of thousands of clinicians on duty at any given period of a day, and any recovery of productivity of this magnitude will create significant efficiencies, cost savings, and result in better patient care for our veterans.

AAIP is directly aligned with the Department's E-Sign initiative. Starting in FY 2005, E-Sign oversight has been transferred under the purview of AAIP. As AAIP implements E-Sign technology, VA will make significant improvements in the use of E-Sign technologies that will streamline veteran services and reduce processing costs incurred by VA. As a net result, this should be dramatically reflected in VA's Government Paperwork Elimination Act and Government Performance and Results Act reporting.

VA currently has several hundred thousand users of computer systems, many with their own separate accounts and passwords. This creates a tremendous account and password burden on VA to operate systems day-to-day. Through AAIP's use of smart cards, VA is setting a progressive architecture and strategy that will improve password management. Smart cards do not require 90 day password rotation, and we have established criteria to implement single sign on (SSO) technologies, minimizing the number of passwords the users have to remember, while leveraging the inherent security of smart cards.

AAIP conducted a detailed analysis of physical access control systems, as they apply to the use of a smart card that is enabled for building access control. Findings indicate that VA could achieve several million dollars in annual cost avoidance through a more efficient strategy related to physical access control system operations.

During FY 2004, the AAIP staff negotiated an enterprise site license with ActivCard for smart card middleware and management software for $12 million, structured into a 4 year lease. The street price of the software is projected at $52 million, resulting in a significant savings.

Internally, VA's Office of the Inspector General (OIG) has identified that AAIP will make a significant contribution towards addressing the finding of "material weakness" and the program will be central to addressing HIPAA security considerations. In addition, this project has been briefed to the national Labor Unions for VA, and has been received favorably. The Labor Unions believe that the employees should have an official ID card and that other derived benefits improve the efficiency of VA.

Externally, over the past 12 months, the Government Accountability Office (GAO) has consistently communicated positive findings related to AAIP and the smart card program. GAO suggested that VA speed up the deployment process from the original 42 month deployment period. VA now has an 18 month deployment period identified in the project planning documents.

AAIP is currently conducting a pilot with the E-Authentication E-Government Initiative, managed by the General Services Administration (GSA), which will test the use of smart cards and public key infrastructure (PKI) credentials against agency systems. This project directly supports the President's Management Agenda, and VA is pleased to act as a leader in this area of government.

VA staff assumed leadership over the Shared Service Provider (SSP) Subcommittee of the Federal Identity Credential Committee (or FICC), acting as the Chair. Starting in September 2003, through the collaborative efforts of the National Institute of Standards and Technology (NIST) and other agencies, the SSP Subcommittee established the evaluation criteria to successfully publish a listing of qualified managed PKI service providers that are available to all federal agencies. As a result, the Federal Government now has a core list of authorized PKI managed services providers, directly supporting the Federal Identity Credentialing Committee chartered by OMB in July 2003.

In September 2004, VA became one of the first Federal agencies to issue a contract to a federally approved managed PKI service provider under the FICC's SSP program. This activity is directly in line with the vision and spirit of OMB's memorandum entitled "Streamlining Authentication and Identity Management within the Federal Government," dated July 2003.

Various Federal agencies are now approaching VA for assistance and access to documentation, processes, and procedures employed by the project to date. This includes the Department of Defense, Department of Interior, National Aeronautics and Space Administration, and the Department of Transportation. The range of requests spans from access to requirements documents, to program structure and testing methodology. While VA recognizes that other agencies have lessons learned that we can benefit from, we are proud of our successes in this area and our ability to share our experience with other agencies.

From a program management perspective, AAIP is directly aligned with mandates from OMB, the Federal CIO Council, the Federal Identity Credentialing Committee and internal VA publications such as the VA Strategic Plan, the VA's Information Technology Strategic Plan, and the VA Enterprise Architecture documents.

The AAIP staff formulated a detailed, structure prototype process to evaluate the injection of smart cards and PKI into the VA enterprise. The prototype process included eight specific areas: remote access, network access, wireless access, thin client access, web access, database access, legacy access and physical access. The prototypes allowed VA to identify what would work, what would not work, and what changes could be made to achieve functionality.

VA is currently participating in the government smart card aggregate buy of smart cards. Initially, VA will procure approximately 100,000 smart cards based on the new Government Smart Card Interoperability Specification v2.1 (GSC-IS). This procurement is being managed by the General Services Administration, pursuant to guidance from OMB. VA will start to receive these smart cards as early as October 2004. Part of the order includes new generation dual-physical antenna cards. These cards, at select facilities, will support co-existence with the current physical access control systems and the ability to migrate to physical access control systems that are compliant with the new GSC-IS specifications.

During the prototype phase of AAIP, the project established a best practices systems engineering approach where the technology was first tested in a controlled lab environment, and then field tested at VA facilities. Examples include successful testing of AAIP and smart card usage for remote access over the enterprise gateways, integrated smart card logon at approximately 10 separate locations across VA, secure testing of smart card logon with wireless technologies, web access, database, and certain legacy devices. The staff also established evaluation processes for physical access control systems, and now serves as the central resources across VA as facilities plan efforts to move to the new federal GSC-IS standards, based on International Organization for Standardization 14443.

Finally, I believe VA has made great progress regarding this important effort, positioning ourselves to implement a smart card program ahead of the schedule outlined in HSPD 12. I remain committed to implementing a smart card program that provides improved business functionality, increased security, and enhanced service to our nation's veterans.

This concludes my written statement. Thank you, Mr. Chairman, for the opportunity to discuss these important matters. I will be happy to answer any questions you might have.